Some assumption underlying reliability prediction

Taylor, J.R.

Publication date:
1975

Document Version
Publisher's PDF, also known as Version of record

A. E. K. Risø

Risø - M - 1794

Risø - M - 1794

Title and author(s)

Some assumptions underlying reliability prediction

by

J.R. Taylor

Date April 1975

Department or group

Electronics

Group's own registration number(s)

R-3-75

pages + tables + illustrations

Abstract

The whole process of reliability prediction for process plant rests on certain assumptions about the way components and process plant behave. It is important to check if these assumptions hold in practice. In some cases they do not. Where the assumptions do not hold, the normal procedures of failure mode analysis and fault tree analysis must be modified and supplement. Some of the more important assumptions are discussed.

Copies to

Available on request from the Library of the Danish Atomic Energy Commission (Atomenergikommissionens Bibliotek), Risø, DK-4000 Roskilde, Denmark
Telephone: (03) 35 51 01, ext. 334, telex: 43116

FI 25-204

ISBN 87 550 0336 2

SOME ASSUMPTIONS UNDERLYING RELIABILITY PREDICTION

J.R. Taylor - AEK Risø

The whole process of reliability prediction for process plant rests on certain assumptions about the way components and process plant behave. It is important to check if these assumptions hold in practice. In some cases they do not. Where the assumptions do not hold, the normal procedures of failure mode analysis and fault tree analysis must be modified and supplemented. Some of the more important assumptions are discussed here.

Assumption: All important modes and combinations of failure can be predicted and evaluated.

Problem 1 In practice there is a problem, for large process plants, because of the large number of combinations of failures involved. It is a common practice in fault tree analysis to ignore combinations which involve more than three or four failures, on the grounds that these combinations are improbable. But in practice, incidents with up to nine independent failures have been observed. Fig. 1 shows a histogram of multi failure incidents described in nuclear reactor abnormal occurrence reports, and shows that four fold, five fold, and six fold failures are significant. The problem is in some cases even more significant, since multiple failures tend to have relatively more serious consequences.

Partial solution: Event tree and causes consequence analysis techniques reduce the problem, by dividing fault trees up into stages. At each stage in a process, only a few combinations of failures are relevant, because only a few components are involved. Using cause consequence analysis many combinations of failures can be eliminated, either because they are very unlikely, or because they are impossible. For example, in a relatively short batch process, it is often impossible to start the process unless safety equipment is working. In this case, the probability of failure of the safety equipment in a later stage of the process is low, because of the short time available for failure. Attention can therefore be concentrated on combinations of failures in equipment which is not checked at the start of the process.

Problem 2 It may be difficult to discover rare failure modes. This problem becomes particularly important if the rare failure modes affect several pieces of equipment simultaneously, or if they start a cascade of failures in other equipment. In such cases, it becomes important to discover such rare failure modes.

Partial solutions One solution to this problem is to collect a catalogue of failure modes for all types of equipment. Then when a particular component is analysed, all the failure modes which have occurred in similar equipment are investigated, even if the failure modes have never been observed in the particular type of equipment being used.

Another solution is to collect statistical data on higher level groupings of components. For example, with a diesel generator, it may be very difficult to investigate all kinds of failure in fuel supply piping, starter motors, cooling systems, etcetera. But if adequate failure data can be collected for diesel generator systems as a whole unit, these problems are short circuited. Even if some rare failure mode occurs which has never been observed before, it will not be significant compared with other failure modes.

These are only partial solutions, because there are problems such as wiring errors, flooding, fire, water hammer effects, and especially, operator error, where consequences of failure can be widespread, and where it is difficult to establish an adequate statistical basis for "complete system" failure rates.

Assumption Failure rates are reasonably constant, and adequate data can be obtained using reliability data base services.

Problem This is a problem especially for process plant, where special reliability tests are impossible, and where such tests would be irrelevant in any case, because of variations in plant conditions.

To illustrate this problem, fig. 2 shows a table of various causes of failure, again drawn from nuclear reactor abnormal occurrence reports. Particularly as far as design and maintenance errors are concerned, there are large variations from plant to plant. These variations inevitably lead to variations in failure rate from plant to plant.

Solutions One obvious solution is to increase the quantity of failure rate data available, discriminating different stress factors, quality control factors, and perhaps, design quality factors. This solution takes time.

An alternative, at the design stage, is to treat failure rates as random variables, fitting a distribution to the variation of failure rates observed in different situations in practice. Fig. 3 shows an example fitting a log-normal distribution to failure rate data drawn from different types of data base. Then, instead of calculating a single reliability value for a system, a distribution of probability values is calculated.

In many cases, it is not necessary to calculate exact reliability values. It is often possible to decide between two alternative equipment designs, by using limiting values for failure rates (if solution A is better than B, both when failure rates are high and when they are low, then solution A is chosen). Sensitivity analysis can be used to discover those cases in which variation in failure rates is important.

Assumption Separate failures are independent, so that the probability of a double failure can be calculated by taking the product of single failure probabilities.

Problem The assumption is often untrue in practice, because several failures occur simultaneously, as a result of a single cause. Such failures can be called coupled failures. There are many possible causes, and many failure types (fig. 4). If such coupled failures prevent an entire subsystem, such as a safety system, from working, they may be called common mode failures. Coupled failures are especially common when there are several components of the same type in a system. Fig. 5 shows some the numbers of such failures for some component types, compared with the number

of single failures, in a sample of abnormal occurrence reports.

Solutions

The first step in a solution to this problem is to identify the areas where such coupled failures are possible.

By extending failure mode and effects analysis, assuming simultaneous failures in similar components, and checking for common dependency on such things as power supply. it is possible to discover those most of the areas where coupled failure is important. By further analysing specific "wide spread" failure effects such as flooding, power supply overvoltage, fire, missile effects, water hammer, loss of ventilation etc., it is possible to identify most of the remaining possibilities.

Calculation of probabilities for such coupled failures is more difficult.
One can use

1) bounding techniques. The probability of coupled failure must be less than the probability of a single failure.

2) joint sampling from a distribution of failure rates. This means that one treats a hazard rate itself as a random variable with a certain distribution (for example uniform, normal, or log normal, centred around an average hazard rate for the particular component type). Then if two components are at risk, failure rates can be assigned to the two components jointly, so that in the part of the distribution where one component is"good", the other component is also "good". When one component is "bad" the other component is also "bad". In this way one obtains a wider range of probabilities for the double failure.

3) The probability of double failure can be calculated from experience of component behaviour, by collecting such data in addition to the usual single failure data. This approach requires more experience and data than for "independent failure" reliability calculations, but in the cases where coupled failure is common, it appears that this approach may be successful.

References

J.R. Taylor, Design Errors in Nuclear Power Plant, September 1974, Riss-M-1742.

N. Rasmussen et.al., Reactor Safety Study (WASH1400 DRAFT), 1974.

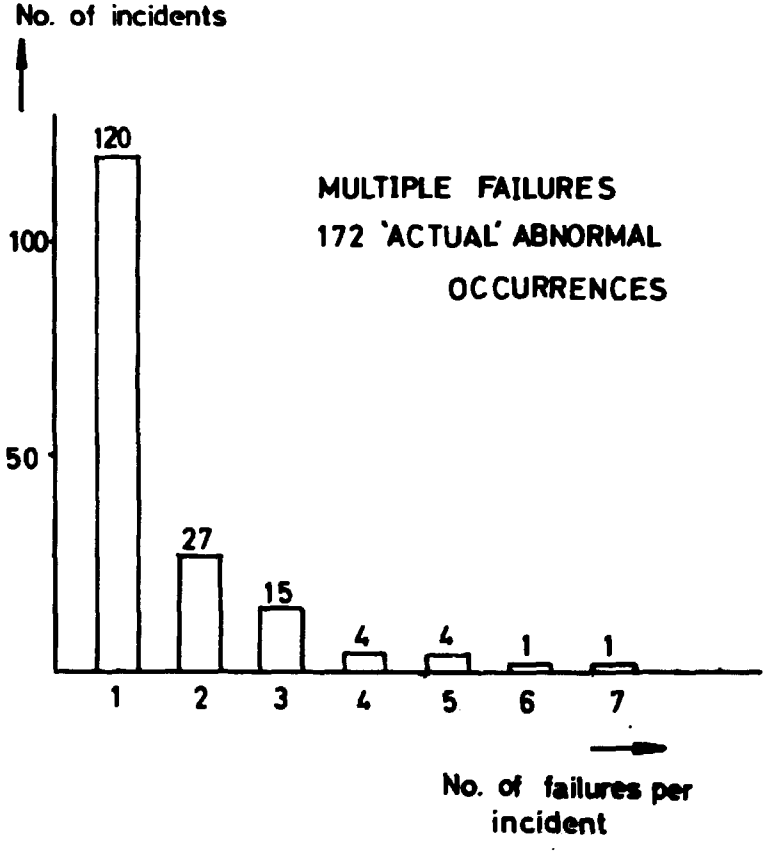

Fig. 1

DESIGN ERROR	36%
RANDOM COMPONENT FAILURE	19 %
MAINTENANCE OR INSTALLATION ERROR	12%
OPERATOR ERROR	11%
PROCEDURAL ERROR	10%
FABRICATION FAULT	0,8%

490 FAILURES

Fig. 2 Failure causes for abnormal occurrences in seven hight water reactors.

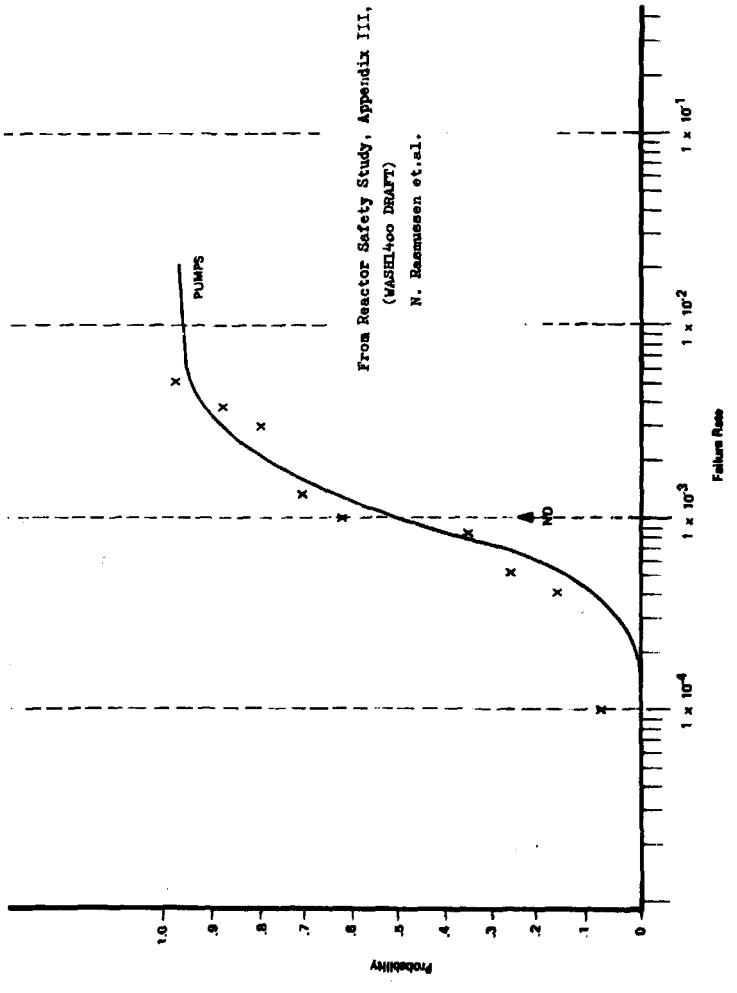

Figure 3. Log-Normal Distribution - Pumps

CAUSES OF COUPLED FAILURE

ENVIRONMENT EFFECTS
EG. VIBRATION, DIRT

DESIGN ERROR OR DEFICIENCY

EXTERNAL PHENOMENA
EG. FIRE, FLOOD

OPERATOR ERROR

CONSTRUCTION AND MAINTENANCE FAULTS

Fig. 4

COUPLED VERSUS SINGLE FAILURES

COMPONENT TYPE	FAILURE TYPE		
	TYPE 1	TYPE 2	SINGLE FAILURE
FLOW SWITCH	1	4	2
MOTORISED VALVE	1	2	6
PRESSURE SWITCH (DRIFT)		11	12
RELAY		3	16

Fig. 5